



Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Department of the Navy

[Docket ID: USN-2013-0038]

Privacy Act of 1974; System of Records

**AGENCY:** Department of the Navy, DoD.

**ACTION:** Notice to add a new System of Records.

**SUMMARY:** The Department of the Navy proposes to add a new system of records in its inventory of record systems subject to the Privacy Act of 1974, as amended. The blanket (k)(1) exemption applies to this systems of records to accurately describe the basis for exempting disclosure of classified information that is or may be contained in the records.

**DATES:** The proposed action will be effective on **[INSERT DATE 31 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless comments are received which result in a contrary determination. Comments will be accepted on or before **[INSERT DATE 30 DAYS FROM DATE PUBLISHED IN THE FEDERAL REGISTER]**.

**ADDRESSES:** You may submit comments, identified by docket number and title, by any of the following methods:

- \* Federal Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- \* Mail: Federal Docket Management System Office, 4800 Mark Center Drive, East Tower, 2nd Floor, Suite 02G09,

Alexandria, VA 22350-3100.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

**FOR FURTHER INFORMATION CONTACT:** Ms. Robin Patterson, Department of the Navy, DNS-36, 2000 Navy Pentagon, Washington, DC 20350-2000 or call at (202) 685-6545.

**SUPPLEMENTARY INFORMATION:** The Department of the Navy notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in **FOR FURTHER INFORMATION CONTACT**. The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on November 21, 2012, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: November 12, 2013.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of  
Defense.

NM03800-1

System name:

Naval Global Maritime, Foreign, Counterterrorism and Counter  
Intelligence Operation Records.

System location:

Primary location: Commander, Office of Naval Intelligence, 4251  
Suitland, MD 20395-2000.

Decentralized segments are located at United States Naval  
organizations worldwide. Official mailing addresses are  
published as an appendix to the Navy's compilation of system of  
records notices.

Categories of individuals covered by the system:

Citizens, lawful permanent residents, and non-US citizens  
associated with vessels, facilities, companies, organizations,  
and ports, or known, suspected, or alleged to be involved in

contraband trafficking (arms, narcotics, and otherwise), illegal migrant activity (smuggling, trafficking, and otherwise), or terrorist activity or piracy in the maritime sector; crew and passengers of maritime vessels defined by the International Maritime Office and various United States and international notices of arrival; individuals identified by the Department of the Navy (DON), other Department of Defense (DoD), Homeland Security, Foreign Allies and Partner personnel during Maritime Interception or Security Operations, vessel boardings, conducting aircraft over-flights, sightings and reports; individuals identified as a potential threat to United States interest in the Maritime Domain sector.

Entities as defined above includes active duty military personnel of the DON including current civilian employees, contract, temporary, part-time, advisory, citizen and foreign nationals located both in the United States and in overseas areas; other Department of Defense employees, and contractors; other named department service members, employees and contractors; other Allied Country, Partnered Country, and Organization service members, employees and contractors; and individuals involved in, or of interest to, foreign intelligence, counterintelligence, counterterrorism, counternarcotics, counter piracy, and counter proliferation

operations or analytical projects, as well as individuals involved in intelligence activities and/or training activities

Categories of records in the system:

Name, nationality, address, email address, home and/or work telephone numbers, cell phone information, identification numbers (e.g. Social Security Number (SSN) and DoD ID Number), Department of Defense number, Passport, Seaman's paper), date of birth, place of birth, photograph, biometrics, personal documents, vehicle license data, relationship to vessels and facilities, relationship to other individuals, companies, government agencies and organizations, involvement with violations of laws and international treaties; associations with vessels involved in contraband, trafficking (arms, narcotics, and otherwise), illegal migrant activity (smuggling, trafficking, and otherwise), unlawful acts within the maritime sector; and associations with other individuals who are known, suspected, or alleged to be involved in contraband trafficking (arms, narcotics, and otherwise), illegal migrant activity (smuggling, trafficking, and otherwise), terrorist activities, or any other unlawful act within the maritime sector.

Information on individuals, companies, vessels, or entities associated with the maritime industry to include: vessel owners,

vessel operators, vessel characteristics, crewmen, passengers, facility owners, facility managers, facility employees; or affiliation with the maritime community, commodities handled, equipment, location certificates, approvals, inspection data, pollution incidents, casualties, and violation of laws and international treaties.

Information on individuals, vessels or entities associated with external watch lists (e.g., law enforcement, biometric, terrorist, and otherwise) on individuals, companies, vessels, or entities associated with threats to the DON, the United States, or United States interest in the Maritime Domain.

Investigative material, correspondence, and other documentation pertaining to investigative or analytical efforts by DON, other United States government agencies, organizations, individuals, and allied or partner countries to identify or counter any foreign intelligence and terrorist threats to the DON, the United States, or United States Interest in the Maritime Domain.

Records relating to ship arrival notifications, crew and passenger lists, boarding reports, threat lists, analytical, operational, biographic, policy, management, training, administrative and operational support related to intelligence,

counterterrorism, counternarcotics, force protection, critical infrastructure protection, research and technology protection, research and development protection, threat analysis, raw intelligence reports and risk assessments.

Authority for maintenance of the system:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. ch 15, National Security Act of 1947, as amended; Executive Order 12333, United States Intelligence Activities; National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13), Maritime Commerce Security Plan for the National Strategy for Maritime Security; 50 U.S.C. ch 36, The Foreign Intelligence Surveillance Act of 1978; DoD Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons; and E.O. 9397 (SSN), as amended.

Purposes(s) :

To carry out the National Plan to Achieve Maritime Domain Awareness by providing an effective understanding of anything associated with the Maritime Domain and identifying threats as early and as distant from the shores of the United States as possible.

To carry out the Global Maritime Intelligence Initiative (GMII) Plan using existing capabilities to integrate all available intelligence regarding potential threats to United States interest in the Maritime Domain.

The maritime intelligence enterprise, the focus of this system, is a federation of departments, agencies, and organizations with a maritime and/or maritime intelligence focus with operational entities frequently being the source of critical information need for intelligence analysis. In the United States this Global Maritime Community of Interest (GMCOI) intelligence enterprise includes entities with the Department of Homeland Security, Department of Defense, Department of State, the Intelligence Community (IC), Department of Justice, Department of Energy, and other United States government departments with responsibilities for international maritime trade, and foreign security and intelligence services.

Internationally, this GMCOI intelligence enterprise includes the entities within the countries allied with the United States or with countries and organizations with bi-lateral partnerships with the United States with responsibility for international maritime trade, security, and intelligence services.



To support Maritime Security Operations (MSO) directed to protect and counter maritime piracy and other threats to U.S. interest in the Maritime Domain.

To document and maintain records on intelligence, counterintelligence, counterterrorism, and counternarcotics operations relating to the protection of national security, DoD personnel, facilities and equipment, to include information systems. To detect, identify, and neutralize foreign intelligence and international terrorist, drug smuggling, or piracy threats to United States interests in the Maritime Domain, the DoD, and United States Naval mission. To maintain records on information operations, foreign intelligence, counterintelligence, counterterrorism, counternarcotics, counterpiracy, counterproliferation, and matters relating to the protection of national security.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974 as amended, these records contained therein may specifically be disclosed outside the DoD pursuant to 5 U.S.C. 552a(b)(3) as follows:

To Federal, State, local, and tribal agencies for the purpose of law enforcement, counterterrorism, counterintelligence, counter-narcotic and piracy activities and Homeland Security as authorized by United States Law or Executive Order, or for the purpose of protecting the territory, people and interests of the United States of America against breaches of security related to DoD controlled information or facilities and against hostile terrorist activities.

To the Immigration and Naturalization Service and the Department of Justice for use in alien admission and naturalization inquiries conducted under section 105 of the Immigration and Naturalization Act of 1952, as amended.

To the Department of State, the Department of Treasury, the Department of Justice, the Federal Bureau of Investigation, the Drug Enforcement Administration, the United States Customs Service, the Bureau of Alcohol, Tobacco and Firearms, and the Central Intelligence Agency for the purpose of collaborating on production of intelligence products and countering terrorist acts.

The DoD Blanket Routine Uses set forth at the beginning of the

Department of Navy's compilation of systems of records notices may apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper and/or electronic storage media.

Retrievability:

Name, SSN, citizenship documentation, biometric data, passport number or vehicle/vessel license data and records.

Safeguards:

Records are stored in office buildings and databases protected by guards, controlled screenings, use of visitor registers, electronic access, and/or locks. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their duties. Passwords and user IDs are used to control access to the system data, and procedures are in place to deter and detect browsing and unauthorized access of electronic files.

Retention and disposal:

General Intelligence Records: Permanent. Retire to the Washington National Records Center (WNRC) when 2 years old, transfer to National Archives and Records Administration (NARA) when 25 years old.

Intelligence Reports: Permanent. Retire to WNRC when 2 years old, transfer to NARA when 25 years old.

Intelligence Products: Retire to WNRC when 2 years old, transfer to NARA when 25 years old.

Intelligence Estimates Records: Permanent. Retire to WNRC when 5 years old, Transfer to NARA in 5-year blocks when 25 years old.

Intelligence Collection Records: Temporary, destroy when 3 years old.

Intelligence Data Base Records: Temporary, destroy when no longer needed to support current requirements.

Paper records are destroyed by shredding, pulping, or burning; electronic records are magnetically erased from the database.

System manager(s) and address:

Commander, Office of Naval Intelligence, 4251 Suitland Road,  
Washington, DC 20395-2000.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries, containing full name and one other personnel identifier (i.e., SSN or date of birth), to Commander, Office of Naval Intelligence, (ONI-22/FOIA), 4251 Suitland Road, Washington, DC 20395-2000.

The system manager may require an original signature or a notarized signature as a means of proving the identity of the individual requesting access to the records.

Record access procedures:

Individuals seeking access to information about themselves contained in this system of records should address written inquiries, containing full name and one other personnel identifier (i.e., SSN or date of birth) to Commander, Office of Naval Intelligence, (ONI-22/FOIA), 4251 Suitland Road, Washington, DC 20395-2000.

The system manager may require an original signature or a

notarized signature as a means of proving the identity of the individual requesting access to the records.

#### Contesting record procedures:

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5E; 32 CFR part 701; or may be obtained from the system manager.

#### Record source categories:

From individuals; DoD records; United States and foreign agencies, organizations or entities; media, including periodicals, newspapers, broadcast transcripts; intelligence source documents/reports; other Navy reports and documents; informants; various Federal, state and local investigative and law enforcement agencies; and other individuals or agencies/organizations that may supply pertinent information.

#### Exemptions claimed for the system:

Investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information may be exempt pursuant to 5 U.S.C. 552a(k)(5) but only to the extent that such

material would reveal the identity of a confidential source.

An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2) and (3), (c) and (e) and published in 32 CFR part 701, subpart G. For additional information contact the system manager.

[FR Doc. 2013-27459 Filed 11/19/2013 at 8:45 am; Publication Date: 11/20/2013]